

ABSTRACT OF THE DISCLOSURE

A stream cipher is provided with a first and a second data bit generators to generate in parallel a first and a second stream of data bits. The stream cipher is further provided with a combiner function having a shuffling unit including a storage structure to generate a pseudo random sequence, by combining the first stream of data bits with at least stochastically generated past values of the first streams of data bits, generated by using the second stream of data bits to stochastically operate the storage structure of the shuffle unit to memorize and reproduce the data bits of the first stream.